2002

Suing the Insecure?: A Duty of Care in Cyberspace

Stephen E Henderson
Matthew E Yarbrough

SUING THE INSECURE?: A DUTY OF CARE IN CYBERSPACE

STEPHEN E. HENDERSON* & MATTHEW E. YARBROUGH**

INTRODUCTION

The Internet, already of major significance throughout much of the globe, is expected to become increasingly pervasive in diverse arenas, from health care, to commerce, to entertainment, and is expected to become increasingly critical to essential infrastructures, including banking, power, and telecommunications. Yet the medium is both inherently and unnecessarily insecure. In particular, today's Internet can be crippled by distributed denial-of-service attacks launched by relatively unsophisticated and judgment-proof parties. Not every computing system involved in such attacks, however, is necessarily without resources. Application of traditional negligence liability, coupled with other government incentives and support institutions, will encourage better security and can be structured to avoid significant disruption of Internet culture.

MAFIABOY AND THE INTERNET

In February of 2000 several major websites were crippled by distributed denial-of-service (DDoS) attacks, including the sites of CNN, Yahoo!, Amazon.com, Dell, and eBay. While the monetary extent of damages is debatable, law enforcement authorities have cited estimates as high as $1.7 billion.[1] Such losses are certainly large enough to justify and make cost-efficient even protracted and complex litigation. As plaintiffs' attorneys know all too well, however, litigation is generally a realistic option only when deep pockets are available. As for the February attacks, the malicious party is not even an adult, let alone one with any significant resources.

The person responsible for crippling these major websites was fifteen years old at the time of the attacks and living with his parents in a Montreal suburb.[2] Known only by his online moniker "Mafiaboy," he managed to bring worldwide attention to the general insecurity of the Internet.[3] This significant insecurity and resulting instability would be of moderate concern if only relatively deep-pocket malevolent actors could exploit it. It is quite another matter when judgment-proof teenagers can do so. Even so, such attacks might still be rare if only that small fraction of teens with exceptional skills could cause such damage.

---

* Visiting Assistant Professor, Chicago-Kent College of Law. J.D. 1999 Yale Law School; B.S. in Electrical Engineering 1995 University of California Davis.

** Principal, Cyberlaw Group, Fish & Richardson P.C. Former Assistant United States Attorney—Head of Cybercrimes Task Force and CTC for the Northern District of Texas. J.D. 1993 SMU School of Law; B.A. 1989 Texas Christian University. The authors would like to thank Michael Rustad and Mark Lemley for their time and insight and Harold Krent and Henry Perritt for their significant encouragement and critique.

1. *See* Christopher Chipello, *Mafiaboy Admits to Charges Linked to Web-Site Attacks*, WALL ST. J., Jan. 19, 2001, at B2.

2. *See* DeNeen L. Brown, *Teen Admits Attacking Web Sites*, WASH. POST, Jan. 19, 2001, at E1; Jon Van & James Coates, *Teenage Hacker Charged*, CHI. TRIB., Apr. 20, 2000, at A3.

3. His true identity remains cloaked pursuant to Canadian law regarding juvenile offenders. *See* Chipello, *supra* note 1. He pleaded guilty to fifty-seven of sixty-seven counts and was sentenced to eight months in juvenile detention and a mandatory $250 charitable donation. *See id. See also* Linda Rosencrance, *Teen hacker "Mafiaboy" sentenced*, COMPUTER WORLD, at http://www.computerworld.com/itresources/rcstory/0,4167,STO63823_KEY73,00.html (Sept. 13, 2001).

Unfortunately, the reality is far different. Many computer attacks, such as the DDoS attacks of Mafiaboy, require only rudimentary skill, and DDoS attacks, though not always as significant as Mafiaboy's, are launched daily.[4] Mafiaboy does not have to be, and in fact is not, a computer genius.[5] Instead, he is one of the growing breed of what are termed "point and click hackers," "script kiddies," "lamers," or "packet monkeys," who know just enough to be dangerous.[6]

Hackers like Mafiaboy do not reinvent the wheel. If one of us "commonfolk" chose to rob a bank, he would not know how to manufacture his own zip gun even if he wanted to. Instead, he would most likely trundle down to the local sporting goods store and purchase a handgun, or, if he had watched a few episodes of crime-drama television, he might purchase one a bit more discreetly. In any case, the hardware is the work of others—the miscreant just pulls, or at least threatens to pull, the trigger.

The online world is no different. Would-be miscreants can browse their favorite hacker websites, downloading diverse attack tools. Or they can participate in hacker chat sessions and beg tools off their more sophisticated counterparts. A hacking tool with a graphical user interface can be used by, relatively speaking, a computer neophyte.[7] That cyberspace allows such costless technique and tool propagation contributes to its attractiveness as a forum for criminal behavior.[8]

This is the current state of the Internet. No one seems to doubt that the Internet will continue to have an increased role in critical infrastructures, including power, banking, telecommunications, transportation, government, and emergency services,

---

4. *See* Kathryn Balint, *'Zombies' Are Latest Hacker-Snatched PCs*, SAN DIEGO UNION-TRIB., Apr. 8, 2001, at A1; Robert Lemos, *Study: Sites Attacked 4,000 Times a Week*, CNET NEWS, *at* news.cnet.com/news/0-1003-200-6006924.html (May 22, 2001); John Markoff & John Schwartz, *Expert Says Windows XP Aids Vandals*, N.Y. TIMES, June 4, 2001, at C7, *available at* www.nytimes.com/2001/06/04/technology/04FLAW.html. Some "hacktivists" utilize DDoS attacks as the cyber-version of a street demonstration, although they attempt to differentiate their actions from those of the Mafiaboy-variety. *See, e.g.*, Jeffrey Benner, *Hacktivists Target Trade Summit*, WIRED NEWS, *at* www.wired.com/news/politics/0,1283,43137,00.html (Apr. 20, 2001); Elizabeth Clark, *Flower Power Cyber Style*, NETWORK MAG., May 1, 2000, at 20.

5. *See* Brown, *supra* note 2; *"Mafiaboy" Pleads Not Guilty to 64 New Charges Related to Hacking*, HOUS. CHRON., Aug. 4, 2000, at B4; Van, *supra* note 2; Ted Bridis & Christopher J. Chipello, *How Mounties Got Their Man in Hacker Case*, WALL ST. J., Apr. 20, 2000, at B1; Graeme Hamilton, *Mafiaboy Pleads Guilty to Online Attacks*, NAT'L POST, Jan. 19, 2001, at A6, *available at* 2001 WL 4435560.

6. Mafiaboy is certainly not the only script kiddie interested in distributed denial-of-service attacks. *See, e.g.*, Scott Berinato, *The Year of the Killer Hackers*, PC WEEK, Dec. 17, 2000, at 1. According to one security professional, "[t]here are a high level of DDoS agents out there right now, on the order of tens of thousands of servers in zombie configuration." *Id.* Microsoft was the victim of a highly-publicized DDoS attack in early 2001. *See Hackers Shut Down Array of Microsoft-Owned Web Sites*, HOUS. CHRON., Jan. 26, 2001, at B3; Barbara Rose, *Hacker Attacks on Microsoft Stir Fears Copycat Assaults May Surface*, CHI. TRIB., Jan. 27, 2001, at B1; Ted Bridis & Rebecca Buckman, *Microsoft Lays 2nd-Day Woes on Hackers*, WALL ST. J., Jan. 26, 2001, at A3. Other examples are given throughout this article.

7. For an example of such a tool, see http://www.sub7.org (last visited Jan. 31, 2002). The competent hackers who write such tools are, in hacker parlance, the "eLite." Needless to say, the "script kiddies" are not fond of the terminology. *See* Michelle Delio, *Call Them Kiddies? Watch Out*, WIRED NEWS, *at* www.wired.com/news/culture/0,1284,41866,00.html (Feb. 16, 2001). Examples of readily available DDoS tools are Trin00, TFN (and its upgrade TFN2k), and Stacheldraht. An internet search of any of these terms will locate information on these tools. A hack is described at Thomas C. Greene, *How to Hack into Microsoft: A Step by Step Guide*, THE REG., *at* www.theregister.co.uk/content/archive/14344.html (Oct. 31, 2000).

8. In other words, one who builds a counterfeit mint cannot costlessly allow all other would-be-criminals, wherever located, free and unlimited access to his mint, and any sharing limits his own use. The world of digital data knows no such limitations, at least unless they are artificially and intentionally imposed.

yet it remains incredibly vulnerable to attack by judgment-proof, unsophisticated parties. How is such a world to be secured?

In part the only answer will be the constant struggle of "technological warfare." Just as new vulnerabilities will consistently and constantly be discovered, so will new defenses. Some Internet systems do utilize and maintain robust encryption, firewalls, intrusion detection, and other "defense" technology.[9] Such defenses are increasing in sophistication daily, including those designed to defend against denial-of-service attacks.

There remains, however, a fundamental weakness inherent to today's Internet. While the Internet's genesis, the Department of Defense's ARPANet, was useful to relatively few, today's Internet is of great use to so many because it is easy to use and its content is incredible in both size and scope.[10] That "anyone" can be an Internet "publisher" is what many find so attractive in the medium. By the same token, that "anyone" can be on the Internet is also what fosters "point-and-click" DDoS attacks.

A denial-of-service attack can be very simple and is not restricted to the online world. If Hillary Clinton established a single-line 1-800 number for campaign contributions, and Rick Lazio called that number all day long and hung up upon connection—or, even better, had a computer do this for him—that would be an effective denial-of-service attack. Legitimate callers would be unable to access the service, and therefore would be unable to make contributions.

A *distributed* denial-of-service attack merely adds additional sources. Miffed that legitimate callers are able to get through in the slight time it takes to redial after hanging up, Lazio might enlist several friends to join him, repeatedly dialing in and hanging up. Once again, it would be that much more efficient to set a number of computers to the task. This is a distributed denial-of-service attack.[11]

When two computers are connected, they necessarily (*i.e.* by definition) have some manner and means of communicating. The Internet, a large collection of interconnected computer networks, is useful precisely on account of this ability to communicate. There may be restrictions on what information a computer will accept—as indeed this is how firewalls attempt to keep out viruses and other malicious content—but there will be some legitimate communication, even if only to receive an authentication request in return.[12]

This is all that is required to make denial-of-service attacks possible on the Internet, as indeed they are possible on all communication networks.[13] If the attacker does not disguise his location, the target can respond to the continual requests by

---

9. For information on such defenses, see BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 188-202 (John Wiley & Sons, 2000).

10. ARPANet, the first packet-switched computer network, began operation in 1969. For a history of the Internet, see Barry M. Leiner et al., *A Brief History of the Internet*, *at* www.isoc.org/internet/history/brief.html (Nov. 18, 2001). An entire list of Internet histories is available at www.isoc.org/internet/history.

11. In 1985 and 1986, Jerry Falwell's toll-free number was subjected to a distributed denial-of-service attack dubbed the "Falwell Game." *See Falwell Alleges Phone Game*, WASH. POST, Feb. 23, 1986, at B3; *Falwell Thinks He Has Way to Win Phone Tie-Up 'Game'*, ATLANTA J. & CONST., Feb. 24, 1986, at A3.

12. The Internet was designed on the "end-to-end" principle that all data should be treated generically, but only the most strident would fault the use of firewalls and other common technologies that today violate this principle. *See Upgrading the Internet*, ECONOMIS, Mar. 24, 2001, at 33.

13. For more information on denial-of-service attacks, see Schneier, *supra* note 9, at 38-39, 181-84.

routinely and immediately denying all further requests, of whatever nature, from that source. If the attacker can effectively disguise his location, however, then such a response is not possible.

Moreover, a distributed denial-of-service attack is more threatening and much more difficult to defend against.[14] An attacker such as Mafiaboy will first hack into a significant number of computers and place code on those computers that he will later use in his attack. These third-party intermediaries are often termed "zombies" or "slaves."[15] Once again, there are automated tools that allow relative neophytes to accomplish this task.[16] Mafiaboy's target of choice for zombies was universities,[17] which are often insecure and have a significant amount of computing power sitting idle at any given time.[18] When the attacker is ready to attack, he signals the zombies, and they all bombard the victim.[19]

While Mafiaboy and other such attackers may be judgment-proof, the zombies are not necessarily lacking in assets.[20] The greater the number of zombies used, the larger the class of potentially deep pockets. The issue for victims therefore becomes, is there some way in which to recover from the intermediaries?

THE LAW OF NEGLIGENCE

While the zombies lack criminal intent, they may have been knowingly insecure in the face of a well-known threat. In order to be made whole, the victim might therefore seek recovery in tort. The common law doctrine of negligence is traditionally divided into four components: (1) a legal duty, (2) a failure to conform one's conduct to the required standard of care, (3) causation, and (4) actual damage.[21]

Although there is little jurisprudence on the application of these components to the realm of modern computing, the third and fourth elements are unlikely to be unusually contentious. For example, although parties will continue to debate the extent of damage, that debate will not be different in kind than the debate in a non-

---

14. According to some experts, there is no defense available; the potential for the attack is inherent in the medium. *See, e.g., id.* at 185. While some are more optimistic, there is no doubt that the DDoS attack is not going to be relegated to the history books any time soon—any technical solution will lead attackers to develop a more sophisticated attack in the ever-evolving technological warfare of the Internet. *See* Robert Lemos, *DDoS Attacks—One Year Later*, ZDNET NEWS, *at* http://www.zdnet.com.com/2110-11-527987.html (Feb. 6, 2001); Hiawatha Bray, *Stopping Internet 'Zombies' In Their Tracks*, BOSTON GLOBE, Mar. 12, 2001, at C1. Newer variants, including those utilizing "pulsing zombies," are described in Michelle Delio, *New Breed of Attack Zombies Lurk*, WIRED NEWS, *at* www.wired.com/news/technology/0,1282,43697,00.html (May 11, 2001).

15. They are also referred to as "Bots" or "IRC Bots."

16. *See Denial of Service Attacks Dog Top Sites with New Tricks*, CHI. TRIB., Mar. 2, 2000, at 1, *available at* 2000 WL 3668812. For more information on DDoS attacks, see Steve Gibson, *The Strange Tale of the Denial of Service Attacks Against GRC.com*, *at* grc.com/dos/grcdos.htm (Aug. 31, 2001).

17. *See* Hamilton, *supra* note 5.

18. *See Hackers Target College Computers*, FINDLAW, *at* http://www.nettime.org/nettime-lat.w3archive/200106/msg00007.html (June 1, 2001).

19. Attackers not only use zombies because adding sources increases attack effectiveness, but because it makes it more difficult to trace the ultimate source of the attack.

20. Moreover, while the attacker may be effectively unreachable in some third-world country, the zombies and their assets may be subject to the jurisdiction of local courts.

21. *See, e.g.*, 57A AM. JUR. 2D *Negligence* § 6 (1989).

computer related negligence action.[22] The first and second components, however, are likely to be the focus of significant litigation in the near future, because neither courts nor legislatures have established the scope of legal duty in cyberspace, nor have they established the extent of said duty.

The issue in a distributed denial-of-service attack is whether a "slave" or "zombie" system is liable to the victim. Given the high-profile nature of recent DDoS attacks, it is absolutely foreseeable that some third party can and will use insecure systems to harm other systems.[23] Therefore, the courts will soon be called on to decide whether zombies owe a duty of care to other Internet systems, and, if so, what is the extent of that duty.

DUTY OF CARE

As is generally the case in "stranger torts,"[24] contractual liability is not available to DDoS victims. For example, although software manufacturers attempt to waive essentially all liability in shrink-wrap and other contracts, it is at least theoretically possible for a purchaser to demand contractual protection for any damage caused by faulty programming. In the case of a DDoS attack, the victim may have had no previous interaction with either the attacker or the zombies, and therefore such contractual liability is impossible.[25]

It is therefore necessary to impose some measure of negligence liability if DDoS victims are to be made whole. According to the *Restatement (Third) of Torts: General Principles* (Discussion Draft 1999), "[a]n actor is subject to liability for negligent conduct that is a legal cause of physical harm."[26] DDoS and other propagated attacks certainly cause "physical harm," as that term is used to include

---

22. The element of causation could be contentious if one considers certain issues herein treated under "duty of care" as issues of causation. Because it is merely a difference of semantics what one "labels" the issue, however, causation will be considered straightforward (the victim would not have been harmed but for the insecurity and the harm was foreseeable), and duty of care the more contentious and unclear issue.

A potential caveat is whether even but for causation can be demonstrated, given that the nature of today's Internet is one of fungible replacements in terms of insecure systems. In other words, there are so many potential zombies available, a zombie might argue that the victim would have been harmed regardless of how secure its system was—the attacker would merely have chosen another intermediary in its place. If courts decide there is a general duty and standard of care as to Internet security, however, it would not be reasonable to argue one should not be liable merely because many others are just as flawed. After all, the standards of an entire industry may be legally unacceptable. *See, e.g., The T.J. Hooper*, 60 F.2d 737, 740 (2d Cir. 1932).

23. Mafiaboy's exploits were certainly not the first denial-of-service attacks to generate significant publicity. An earlier example is the attack on fbi.gov and other government sites in retaliation for the indictment of a member of the hacker group Global Hell. *See* Chris Taylor, *Geeks v. G-Men: A Virtual Shooting War Breaks Out Between Hackers and the FBI. Are the Kids Really Worth the Trouble?*, TIME, June 14, 1999, at 64. Other DDoS attacks are mentioned in later portions of this article.

24. The term "stranger torts" is used merely to refer to torts between strangers. While acquainted parties may form contracts and seek enforcement thereof, they may also seek recovery in tort.

25. It would not necessarily remain impossible were the entire nature of the Internet to change. For example, an architecture could be created that would require contractual guarantees, bonding, and other such requirements before allowing a "connection" to the Internet. Although this would almost entirely defeat the "end-to-end" principle on which the Internet is based, as Lawrence Lessig has persuasively argued, it is a mistake to presume the Internet of tomorrow will necessarily resemble the Internet of today. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999).

26. RESTATEMENT (THIRD) OF TORTS: GENERAL PRINCIPLES § 3 (Discussion Draft 1999).

both personal injury and property damage.[27] This definition of negligence is tempered, however, by requiring a duty:

> Even if the defendant's negligent conduct is the legal cause of the plaintiff's physical harm, the [defendant] is not liable for that harm if the court determines that the defendant owes no duty to the plaintiff. Findings of no duty are unusual, and are based on judicial recognition of special problems of principle or policy that justify the withholding of liability.[28]

While the Draft Restatement recognizes that duty is more likely to be an issue when the allegedly negligent conduct involves "setting the stage or creating the opportunity for the tortious misconduct of some third party,"[29] its assertion that a finding of no duty should be rare is persuasive. While courts often term their analysis one of "duty," this analysis is rarely meaningful and often smuggles in several elements that are more properly regarded as elements of "standard of care."[30] With regard to Internet security, there is no persuasive reason not to require a duty of care. Malicious uses of insecure Internet systems are legion, and there is no meaningful policy reason to treat failure to take precautions in the online world any differently than failure to take precautions in the "brick and mortar" world.

If a car is recalled on account of an unpredictable yet frequent tendency to lose control, it would be negligent to knowingly continue to drive the vehicle without having it serviced. Likewise, though more unlikely, if the vehicle was designed in such a way that kicking the tire caused it to burst without warning at any time within the hour, and such "attacks" were frequent and publicized, including their harm to innocent bystanders, it would be negligent not to remedy the situation. Yet many computer systems are knowingly insecure, in part on account of failure to install readily available software patches.[31] There is no reason not to impose a duty of care on the "information highway" akin to that imposed on the asphalt highway.

The DDoS question of duty is somewhat analogous to another situation that courts are currently confronting, namely, attempts to hold gun manufacturers and distributors liable for handgun deaths. In the case of a gun, the person who uses the

---

27. *See id.* cmt. a. This damage includes not only harming physical assets, such as via deletion of data, but also inability to serve customers. The identical distinction applies in the "brick and mortar" context. If one breaks the shopkeeper's window glass, such action damages the shopkeeper. If an individual beats up every person attempting to enter the establishment, or otherwise blocks entry, such actions likewise damage the shopkeeper. While there will continue to be significant debate regarding precisely what qualifies as "damage" in the computer context, just as there is significant debate regarding the economic loss rule in the "brick and mortar" context, the precise contours of that definition are not necessary to determine whether some liability should exist.

28. RESTATEMENT (THIRD) OF TORTS § 6 (Discussion Draft 1999).

29. *Id.* cmt. d.

30. *See id.* cmts. a, c, e. The risk-utility factors used in Nebraska are instructive: (1) the magnitude of the risk, (2) the relationship of the parties, (3) the nature of the attendant risk, (4) the opportunity and ability to exercise care, (5) the foreseeability of the harm, and (6) the policy interest in the proposed solution. *Knoll v. Bd. of Regents*, 601 N.W.2d 757, 761 (Neb. 1999). *See also* City of Philadelphia v. Beretta U.S.A., Corp., 126 F. Supp. 2d 882, 898-902 (E.D. Penn. 2000); Hamilton v. Accu-Tek, 62 F. Supp. 2d 802, 818-27 (E.D.N.Y. 1999).

31. *See, e.g., Denial of Service Attacks Dog Top Sites with New Tricks*, *supra* note 16; Balint, *supra* note 4; Brock N. Meeks, *FBI Says Net Companies Targeted by Extortion Scheme: Officials Say Firms Must Protect Credit Card Numbers Better*, MSNBC, *at* www.msnbc.com/news/541331.asp (Mar. 8, 2001) (discussing successful attacks exploiting well-known vulnerabilities for which patches exist). Some estimate that over ninety-nine percent of all Internet attacks could be prevented if system administrators used the most current versions of software. *See* Schneier, *supra* note 9, at 210-11.

weapon is generally clearly liable to the victim, but that person is often either impossible to locate, is judgment-proof, or both. Therefore the goal is to hold liable the manufacturer or distributor of that weapon, who made it accessible to the ultimate bad actor.[32] Although cases to date have achieved only minimal success, as the relevant legal arguments become more common and therefore seem less novel, courts are likely to allow the potential for such liability.[33]

Similarly, in the case of a DDoS attack, the person who uses the "weapon" (*i.e.* the zombie) is generally clearly liable to the victim, but that person is often either impossible to locate, is judgment-proof, or both. Therefore, the goal is to hold liable the person or entity responsible for making that weapon accessible to the ultimate bad actor. Further, unlike in the handgun context, there are rarely significant intermediaries, if any, between the entity or individual through which the ultimate bad actor directly obtains access and the allegedly responsible party.[34] While the specific facts of every individual case should be carefully considered in determining liability, there is no reason some duty of care should not be imposed.

STANDARD OF CARE

That there should be some duty of care does not answer what the extent of that duty should be. Because some insecurity will necessarily exist in all Internet systems,[35] absolute security cannot be required, and personal users certainly should not be required to establish military-grade systems. Instead it will be necessary to determine when conduct is deemed to pose an unreasonable risk of harm, which is often said to require that standard of care that a reasonably prudent person would use under the circumstances. According to the Draft *Restatement (Third) of Torts*,

> [a]n actor is negligent in engaging in conduct if the actor does not exercise reasonable care under all the circumstances. Primary factors to consider in ascertaining whether conduct lacks reasonable care are the foreseeable likelihood that it will result in harm, the foreseeable severity of the harm that

---

32. Similarly, one may be found negligent for failure to secure a firearm from access by others. *See, e.g.*, L.S. Rogers, Annotation, *Liability of Person Permitting Child to Have Gun, or Leaving Gun Accessible to Child, for Injury Inflicted by the Latter*, 68 A.L.R. 2d 782, 785 (1959).

33. For information on some of these cases, see Francis M. Dougherty, Annotation, *Handgun Manufacturer's or Seller's Liability for Injuries Caused to Another by Use of Gun in Committing Crime*, 44 A.L.R. 4th 595 (1986); Colin K. Kelly, Note, *Hamilton v. Accu-Tek: Collective Liability for Handgun Manufacturers in the Criminal Misuse of Handguns*, 103 W. VA. L. REV. 81 (2000). *See also* Sharon Walsh, *Campaign Heats Up Against Gun Firms*, WASH. POST, Apr. 12, 1999, at A1; Sharon Walsh, *For Plaintiffs, the Difficulty of Obtaining Monetary Awards*, WASH. POST, Apr. 12, 1999, at A14; Hamilton v. Accu-Tek, 62 F. Supp. 2d 802 (E.D.N.Y. 1999), *question certified by* Hamilton v. Beretta U.S.A. Corp., 222 F.3d 36 (2d Cir. 2000), *certified question accepted by* 738 N.E.2d 1055 (N.Y. 2000), *certified question answered by* 750 N.E.2d 1055 (N.Y. 2001); City of Philadelphia v. Beretta U.S.A., Corp., 126 F. Supp. 2d 882 (E.D. Penn. 2000).

34. "[T]he connection between defendants, the criminal wrongdoers and plaintiffs is remote, running through several links in a chain consisting of at least the manufacturer, the federally licensed distributor or wholesaler, and the first retailer. The chain most often includes numerous subsequent legal purchasers or even a thief." *Hamilton*, 750 N.E.2d at 1061-62. In other words, in the handgun context the shooter may have purchased the gun from A, who stole it from B, who purchased it from C, who purchased it from D, and D is being sued. In the DDoS context the "shooter" hacked into a system owned by A and maintained by B; A (and potentially also B) is being sued.

35. This is true of all known systems. *See* RESTATEMENT (THIRD) OF TORTS § 4 cmt. h (Discussion Draft 1999).

> may ensue, and the burden that would be borne by the actor and others if the actor takes precautions that eliminate or reduce the possibility of harm.[36]

These "primary factors" are essentially those enunciated by Learned Hand in *United States v. Carroll Towing Co.*[37] According to *Carroll Towing*, conduct is negligent if the cost of prevention would have been less than the probability of harm multiplied by the gravity of the resulting injury.[38] Unfortunately, in relatively new and developing sectors such as the Internet, such analysis can be quite difficult on account of a lack of empirical data.

One useful source in determining standard of care is industry custom:

> (a) The actor's compliance with the custom of the community, or of others in like circumstances, is evidence that the actor's conduct is not negligent, but does not preclude a finding of negligence.
> (b) The actor's departure from the custom of the community, or of others in like circumstances, in a way that increases risks is evidence of the actor's negligence but does not require a finding of negligence.[39]

Thus, while "ordinary care" is often "reasonable care," it is not always so. All, or most, of the members of a relevant group may have lagged behind what is reasonable.[40] This may be especially true in new or evolving sectors of society, where reasonable customs have yet to take root. Further, for internally divergent sectors such as the Internet, it is crucial that courts carefully distinguish the factual circumstances of each case. While both an individual user utilizing a cable modem to maintain a web page of family photos and a university utilizing a network of hundreds of workstations may be permanent residents of the Internet, what might be a reasonable amount of precaution by one would almost certainly be insufficient on the part of the other.

"Ordinary care" may often become, over time, "reasonable care" as parties react to the threat of, and actuality of, negligence lawsuits. If a whole class of victims fails to bring such lawsuits, however, this natural progression will be delayed. Lawsuits against DDoS zombies, or other insecure intermediaries such as those that pass on viruses and worms, undoubtedly will soon find their way to the courthouse. That they have not done so to date is surprising but is in large part due to victim reluctance to further degrade the perception that the Internet is at least somewhat secure and fear of becoming tomorrow's defendant. In other words, just as companies are reluctant to report their own security breaches for fear of negative publicity and attracting other hackers,[41] victims of DDoS and other attacks are

---

36. RESTATEMENT (THIRD) OF TORTS § 4 (Discussion Draft 1999).
37. 159 F.2d 169, 173 (2d Cir. 1947).
38. *See id.*; RESTATEMENT (THIRD) OF TORTS § 4 cmts. d, e (Discussion Draft 1999).
39. RESTATEMENT (THIRD) OF TORTS § 11 (Discussion Draft 1999).
40. *See id.*; *see also* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It may never set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.").
41. *See, e.g.*, Michelle Delio, *Brit Cops Tackle E-Thievery*, WIRED NEWS, *at* www.wired.com/news/business/0,1367,43171,00.html (Apr. 19, 2001). Some estimate as many as eighty percent of security incidents go unreported.

reluctant to sue arguably responsible intermediaries because they fear they may themselves be tomorrow's insecure intermediaries.

Courts may also look to a standard of care set by legislation.[42] While there are no generally applicable legislative mandates of Internet security, there is both federal and state sector-specific legislation. For example, the proposed security regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[43] mandate significant security.[44] Regulated entities must

> maintain reasonable and appropriate administrative, technical and physical safeguards—
> (A) to ensure the integrity and confidentiality of the information;
> (B) to protect against any reasonably anticipated—
> (i) threats or hazards to the security or integrity of the information; and
> (ii) unauthorized uses or disclosures of the information; and
> (C) otherwise to ensure compliance with this part...by officers and employees.[45]

While technologically neutral, these proposed regulations require significant security measures, which the regulations divide into four categories: administrative procedures (manage the selection and execution of security measures, including relevant management of personnel); physical safeguards (protect computer systems, buildings, and related equipment from fire, natural disaster, and intrusion); technical security services (monitor and control information access and integrity); and technical security mechanisms (protect data in transmission).[46] Included in the proposed regulations is a detailed matrix of requirements and implementations for

---

See Protecting America's Critical Infrastructures: How Secure are Government Computer Systems?: Hearing Before the Subcomm. on Oversight and Investigations of the House Comm. on Energy and Commerce, 107th Cong. (statement of Sallie McDonald, Assistant Commissioner, USGSA), *available at* http://www.nist.gov/hearings/2001/govcomp.htm (Apr. 5, 2001).

42. *See* RESTATEMENT (THIRD) OF TORTS § 12 (Discussion Draft 1999).

43. Pub. L. 104-191, 110 Stat. 1936.

44. The Act is broad in scope, including all of the following elements. Final regulations concerning the majority of statutorily specified transaction and code sets—intended to improve efficiency by standardizing electronic exchange of administrative and financial health care transactions—have been promulgated, and compliance is required by October 16, 2002, with a one-year extension for small health plans. *See* aspe.hhs.gov/admnsimp/bannertx.htm; aspe.hhs.gov/admnsimp/faqtx.htm; aspe.hhs.gov/admnsimp/faqcode.htm; *Health Insurance Reform: Standards for Electronic Transactions; Correction*, 65 Fed. Reg. 70,507 (Nov. 24, 2000); *Health Insurance Reform: Standards for Electronic Transactions*, 65 Fed. Reg. 50,312 (Aug. 17, 2000) (to be codified at 45 C.F.R. pts. 160, 162). There are still no final regulations with regard to national provider identifiers, national employer identifiers, or national health plan identifiers. *See* aspe.hhs.gov/admnsimp/bannerid.htm. "Final" regulations governing medical privacy were promulgated on December 28, 2000, and became effective as of April 14, 2000, making the compliance date April 14, 2003, with a one-year extension for small health plans. *See* aspe.hhs.gov/admnsimp/bannerps.htm; *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164); *Standards for Privacy of Individually Identifiable Health Information*, 66 Fed. Reg. 12,738 (Feb. 28, 2001) (to be codified at 45 C.F.R. pts. 160, 164). Proposed security regulations were promulgated on August 12, 1998, but final regulations are still pending. *See* aspe.hhs.gov/admnsimp/bannerps.htm; *Security and Electronic Signature Standards*, 63 Fed. Reg. 43,242 (Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142).

45. 42 U.S.C. § 1320d-2(d)(2) (Supp. V 1999).

46. *See Security and Electronic Signature Standards*, 63 Fed. Reg. 43,250, 43,266-68 (Aug. 12, 1998) (to be codified at 45 C.F.R. pt 142).

each of these four categories.[47] Knowing violation may result in significant criminal penalties.[48]

The financial sector is similarly regulated by security provisions contained in the Gramm-Leach-Bliley Act of 1999 (GLBA).[49] Section 501(b) of GLBA requires regulated institutions to

> establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[50]

Five relevant federal agencies have promulgated final regulations pertaining to GLBA's security provisions.[51] Although the regulations are not as detailed as the relevant HIPAA regulations, they too require assessment, training, testing, and implementing of security measures.[52] Unlike HIPAA, however, GLBA provides only administrative remedies for security infractions.[53]

While both HIPAA and GLBA mandate security, they do so in order to protect the confidentiality and integrity of data stored on covered entities' computer systems. In the DDoS context, the victim instead seeks to hold a zombie system liable for failure to secure its system against use as a harmful tool by a malicious third party. In other words, whereas HIPAA and GLBA are concerned with security on account of the data contained on a system, the issue in DDoS is security in order to make difficult and costly malicious use by a third party, regardless of the system's data content.

According to the *Draft Restatement (Third) of Torts*, "[a]n actor is negligent if, without excuse, the actor violates a statute that is designed to protect against the type of accident the actor's conduct causes, and if the accident victim is within the class of persons the statute is designed to protect."[54] The victim of a DDoS attack is *not*

---

47. *See id.* at 43,251, 43,253, 43,254, 43,255, 43,269-71.

48. *See* 42 U.S.C. § 1320d-5, 1320d-6 (Supp. V 1999).

49. Pub. L. No. 106-102, 113 Stat. 1338. The Act is also commonly termed the "Financial Modernization Act of 1999" or the "Financial Services Modernization Act."

50. 113 Stat. 1437, codified at 15 U.S.C. § 6801(b) (Supp. V 1999).

51. *See* www.privacyheadquarters.com/timeline.html (last visited Nov. 20, 2001); *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. 8616 (Feb. 1, 2001) (to be codified at multiple parts of 12 C.F.R.); *Guidelines for Safeguarding Member Information*, 66 Fed. Reg. 8152 (Jan. 30, 2001) (to be codified at 12 C.F.R. pt. 748).

52. *See, e.g., Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. at 8633. The lack of specificity is causing confusion and contention for those attempting compliance. *See* Rutrell Yasin, *Confusion Rises Over Privacy Law*, TECHWEB, *at* www.techweb.com/wire/story/TWB20010529S0012 (May 29, 2001).

53. *See* GLBA, 113 Stat. 1440, codified at 15 U.S.C. § 6805 (Supp. V 1999).

54. RESTATEMENT (THIRD) OF TORTS § 12 (Discussion Draft 1999). The excuse provisions are contained at section 13. The relevance of *conformance* with a pertinent statute is found at section 14(a): "An actor's compliance with a pertinent statute, while evidence of non-negligence, does not preclude a finding that the actor is negligent under § 4 for failing to adopt precautions in addition to those mandated by the statute."

within the class of persons HIPAA and GLBA are designed to protect, because the victim need not have confidential data stored on the intermediaries' systems.[55] Therefore, violation of the HIPAA or GLBA security standards should not be considered negligence *per se* in the DDoS situation. This is not to say, however, that such security standards are not *relevant* in the DDoS situation. Currently such legislation and accompanying regulations provide the most comprehensive legislative and regulatory discussion of computer security standards. To a jury or court that is only minimally computer literate, these materials will provide at least some guidance on what is technically and economically feasible, at least in some industry sectors. Furthermore, while not true of all HIPAA/GLBA security requirements, many, though intended for data protection, are also relevant to preventing the malicious system use relevant to DDoS. Future plaintiffs are therefore likely to cite the security requirements of HIPAA, GLBA, and similar state statutes as evidence of negligence.

Lastly, it is *not* a defense to liability that damage would not have occurred but for the malicious, and indeed criminal,[56] actions of a third party, where those actions were foreseeable. "The conduct of a defendant can lack reasonable care insofar as it can foreseeably combine with or bring about the improper conduct of the plaintiff or a third party,"[57] even where that improper conduct is "tortious or criminal, or both."[58] As in the case of premises liability, if a given system has been subject to previous attacks, liability for the known insecurity is that much more direct.[59]

Taken in its entirety, this analysis does not, and cannot, fully articulate what standard of care should be applicable in a given case, but it does delimit a number of relevant sources that should be consulted. Those sources must be applied in a factually-sensitive manner: while an individual connected to the Internet via a cable modem may be required to purchase a commercially available personal computer software firewall[60] and to install readily available software patches, a research university connecting hundreds of workstations to the Internet might be required to do significantly more.

EFFECT ON CYBERSPACE(S)

While application of traditional negligence liability will improve Internet security, such common law develops relatively slowly, can vary significantly by jurisdiction, and might have significant unintended effects on Internet utility and

---

55. *See id.* § 12 cmts. f, g.

56. In the case of a DDoS attack, the attacker violates, inter alia, provisions of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994 & Supp. V 1999).

57. RESTATEMENT (THIRD) OF TORTS § 17 (Discussion Draft 1999). *See also id.* § 17 cmt. e: "[T]he defendant's conduct may make available to the third party the instrument eventually used by the third party in inflicting harm."

58. *Id.* § 17 cmt. a. This follows directly from application of a general negligence definition, such as that found at section 4 of the Draft Restatement. *See id.* § 17 cmt. d.

59. *See, e.g.*, Marjorie A. Caner, Annotation, *Liability of Owner or Operator of Shopping Center, or Business Housed Therein, for Injury to Patron on Premises from Criminal Attack by Third Party*, 31 A.L.R. 5TH 550 (1995); RESTATEMENT (SECOND) OF TORTS § 344 (1965).

60. Effective applications only cost about forty dollars. *See, e.g.*, Barry Nance, *Four Personal Firewalls Reviewed*, COMPUTERWORLD, *at* www.computerworld.com/cwi/story/0,1199,NAV47_STO60821,00.html (May 28, 2001).

culture. As Lawrence Lessig has elegantly articulated, cyberspace is really many places, and each of those places has a unique nature determined in part by the architecture of code governing that space.[61] To use Lessig's example, the rules and norms governing users of America Online (AOL) are different from those governing users of the former online legal community Counsel Connect,[62] which are different from those governing users of a given private university network.[63] That all such communities are part of the Internet, utilizing the IP communications protocol, does not mean that all such communities have identical norms, rules, and regulations. This flexibility is an attractive component of cyberspace.

Unfortunately, in the case of attacks that rely only on there being a common communications protocol, such divergence is not relevant. A DDoS attack can be launched from, or can cripple, any community. The systems running Counsel Connect, if hacked, could have been used as zombies to bombard those running AOL, and vice-versa. While different systems may include varying degrees of security to defend against such attacks, their mere presence on the Internet makes them both potential targets and tools.

This congruence has implications for the effect of requiring legal duties of Internet security. Many find the Internet attractive precisely because, relatively speaking, the barrier to entry is low. The lowest cost methods of entry are subject to the architectures, and thus rules, of others. This includes using an analog modem to dial an Internet Service Provider such as AOL, AT&T's Worldnet, or Microsoft's MSN.

Those not willing to be bound by the architectures of others can still establish their own architecture with relatively minimal equipment. A home computer with a cable modem running as an HTTP server can, theoretically, be available to all other Internet users, or at least those users accessing the Internet through an architecture that does not artificially block that content. Like all generally applicable laws, however, the law of negligence can severely restrict this potential.

Questions of "proper" jurisdiction aside, general laws can have enormous impact on cyberspace. For example, it may be true that, were the People's Republic of China, or the United States, to deem all unlicensed Internet servers illegal, perfect enforcement of that law would be impossible. Perfect enforcement, however, is almost never possible and is certainly almost never necessary. Most would-be-users will not make international telephone calls to obtain service. Commercial entities are beholden to generating a profit, and therefore willfully subject themselves to the law lest they defeat that purpose. Further, most users, being unaware of Internet Protocol addresses,[64] can be effectively blocked from accessing certain content merely by

---

61. *See* Lessig, *supra* note 25. While page 82 articulates this principle, the entire book presents its development.

62. Information on AOL is available at www.aol.com. Counsel Connect, an early proprietary online service for lawyers, was formerly available at www.counselconnect.com but is no longer in operation. One of its descendants can be found at www.law.com.

63. *See* Lessig, *supra* note 25, at 66-84.

64. Every system on the Internet is assigned an Internet Protocol (IP) address, which is used in routing packets of data. In the currently mainstream protocol IPv4, the addresses consist of thirty-two binary digits. This allows for over four billion addresses, namely 2^32. *See Upgrading the Internet*, *supra* note 12, at 32. In IPv6, they consist of 128 binary digits, allowing for an enormous number of combinations, namely 2^128. *See id.* at 33.

removing the entries to that content from the relevant domain name servers—it is unnecessary to physically deactivate the renegade systems.[65]

For these and many more reasons, the law has a significant impact on cyberspace.[66] Therefore, were the law even only in the United States to require a stringent standard of care with regard to system security, it would impact cyberspace. In the above example, those wishing to provide a service or express views outside the existing architectures will not only face the relatively minimal cost of purchasing functional computer equipment, but also will face the additional cost of potential liability.[67] The magnitude of this impact will depend on the standard imposed. Requiring all Internet systems to utilize, at a minimum, commercially available software firewalls might not be prohibitive. Likewise, requiring installation of reasonably available software patches might not be prohibitive. Requiring systems to perform effective scans for the presence of renegade programs, such as zombie software, may or may not be prohibitive. Implementing even these relatively limited changes would substantially improve overall Internet security.[68]

While the optimal standard will be difficult to determine and will require adapting both to the benefit of hindsight and changing circumstance, it is important that those articulating any standard carefully consider both its effects and potential manners of mitigating any such effects deemed unfavorable. For example, it may prove to be too confusing, too time-consuming, or both, for the average Internet user to securely maintain any software, including that requiring periodic updates such as virus checkers. If such is the case, rather than, or in conjunction with, imposing liability on average users, the government may want to require, or at least "encourage," internet service providers (ISPs) and application service providers (ASPs) to host such updates and scan users' computers for relevant insecurities.[69] Likewise, manufacturers of insecure software could be required to release and issue security updates via CD-ROMs distributed via mail services, somewhat more akin to product recalls in other sensitive areas, rather than merely post them to relatively obscure websites.[70]

Alternatively, or in addition, the government can create and/or support entities designed to aid user compliance. The federal government in particular supports a

---

65. For more information on IP addresses and domain name servers, see Schneier, *supra* note 9, at 176-81.

66. *See, e.g.*, Patricia Jacobus et al., *Taming the Web: New Technologies, Laws Raise Barriers Online*, CNET NEWS.COM, *at* www.cnet.com/news/0-1005-201-5589627-0.html (Apr. 19, 2001). We see this effect indirectly as well as directly. When Napster-esque systems are made illegal, distributed-architecture Gnuetella-esque systems begin to thrive.

67. Similar situations in the "brick and mortar" world, however, have not justified failure to impose negligence liability, as in the case of mandating auto insurance.

68. *See Denial of Service*, *supra* note 16; Balint, *supra* note 4.

69. Such a model already exists in niche markets. *See, e.g.*, *Gathering Steam: Software Is Migrating from Users' Computers to the Internet*, ECONOMIST, Apr. 14, 2001, at 7 (Software Survey).

70. Some companies are beginning to implement new vehicles for disseminating security patch information. *See, e.g.*, *Microsoft Offers Two New Security Tools*, COMPUTERWORLD, *at* www.computerworld.com/storyba/o,4125,NAV47_STO63091,00.html (Aug. 16, 2001) (discussing the distribution of tools enabling users to scan their systems to determine what security patches should be installed). Additionally they could be required to, or at least encouraged to, ship their products with security features enabled, rather than the default status being disabled. While unsophisticated users may be frustrated by the performance limitations and complications that such features necessarily entail, a default of poor security is not a better option. Whether or not the government requires this change, negligence liability will encourage it.

number of organizations designed to aid computer professionals in maintaining system security. The multi-agency National Infrastructure Protection Center (NIPC), headed by the FBI, is designed to serve as "a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[71] NIPC in turn leads InfraGard, an information-sharing network for law enforcement, academic institutions, and businesses.[72]

A federal government-funded organization with less of a law enforcement bent is the CERT Coordination Center (CERT/CC) operating out of Pittsburgh's Carnegie Mellon University.[73] Established by the Defense Advanced Research Projects Agency following the infamous "Morris" worm,[74] CERT/CC studies and then releases information on Internet security threats, first to the government and select business entities and then to the "public."[75] A similar institution could be funded that would host software patches and other security tools, and provide neophyte-usable instructions, in order to allow the average Internet user to maintain a somewhat secure system.

While courts should consider all of these issues when fashioning the negligence law of cyberspace, they necessarily formulate the law on a case-by-case basis and are institutionally unable to remedy undesirable effects via legislative incentives or the creation of "helper" agencies such as CERTs designed for the average Internet user. Legislators and executives, especially on the federal level, should therefore begin to consider these issues now, before the lawsuits begin to stream to the courthouse. The current dearth of litigation in this area will not—and indeed should not—last, as the Internet must be made more secure if it is to fulfill its perceived destiny. Ultimate resolution of these issues will require the deliberation and intervention of courts and legislatures on the state, national, and potentially even international (treaty) level.

CONCLUSION

As demonstrated by the exploits of Mafiaboy, liability in the DDoS context is a significant issue. Experts predict additional, and potentially much more expansive, DDoS attacks will occur in the near future—it is estimated that from 10,000 to over

---

71. *National Infrastructure Protection Center*, *at* www.nipc.gov (last visited Nov. 20, 2001). NIPC has, however, been somewhat pathetic in execution. *See, e.g.*, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323, *available at* www.gao.gov (Apr. 25, 2001); David A. Vise, *FBI Warns Infrastructure Vulnerable to Cyber-Attacks*, WASH. POST, Mar. 21, 2001, at A16; Patrick Thibodeau, *GAO: NIPC Late on Cyberattack Alerts, Lacks Expertise*, COMPUTERWORLD, *at* www.computerworld.com/cwi/story/0,1199,NAV47_STO60773,00.html (May 22, 2001).

72. *See InfraGard Public Site Main Page*, www.infragard.net (last visited Nov. 20, 2001); David A. Vise, *FBI Takes Aim at Cyber-Crime: Agency Seeks to Enlist Wary Private Sector in Joint Prevention Effort*, WASH. POST, Jan. 6, 2001, at A2.

73. *See CERT Coordination Center*, www.cert.org (last visited Nov. 20, 2001).

74. *See* Press Release, Carnegie Mellon University, *DARPA Establishes Computer Emergency Response Team*, *available at* www.cert.org/about/1988press-rel.html (Dec. 13, 1988).

75. *See* Sam Costello, *CERT to Sell Security Threat Information*, INFOWORLD DAILY NEWS, *at* http://www.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/01/04/19/010419hncert.xml&dctag=security (Apr. 19, 2001). While CERT/CC information is available to "everyone" via the Internet, it is intended for use by the professional and is written accordingly.

100,000 active zombies exist at any one time.[76] These estimates are believable given current attack statistics. Seventy-eight percent of respondents to the 2001 Computer Security Institute (CSI)/FBI Computer Crime and Security Survey reported denial-of-service attacks against their web sites.[77] A team of researchers at the University of California at San Diego recently witnessed 4000 DDoS attacks in each week of a three-week study.[78] While such attacks against commerce are significant, attacks against critical infrastructures such as power grids and emergency services are that much more serious.[79] The FBI, via NIPC, recently issued a renewed warning of denial-of-service attacks in the wake of several recent attacks, including DDoS attacks against the Web sites of CERT/CC and the White House.[80]

It is a virtual certainty that, at least absent legislation restricting them, negligence lawsuits will soon become a regular component of this future. Moreover, while the DDoS context may well lead the way, negligence lawsuits in similar contexts will soon follow. It is only a matter of time before a party whose system is hacked, or who faces liability based on some insecurity in its system (potentially including being a DDoS slave), seeks (and obtains) recovery in negligence from the party that designed or maintained that system, or that designed or maintained that system's software.

Given the common knowledge that computer systems with inadequate security can be compromised, not only compromising the data stored therein but potentially allowing the system to be used for malicious purposes, there should be more discussion of what duties and standards of care should apply. Interested parties would be wise to begin taking security precautions now, as well as to begin advocating their view of what the law should require. A failure to take either action will leave parties at the mercy of judges and juries forced to consider these complicated technical and legal issues as matters entirely of first impression, partially crippled by courts' inherent inability to provide certain remedies.

---

76. *See* Balint, *supra* note 4.

77. *See CSI/FBI Computer Crime and Security Survey*, Spring 2001, at 4, *available at* www.gocsi.com.

78. *See* Lemos, *supra* note 4. These 13,000 witnessed attacks do not account for the potentially numerous unwitnessed variants. *See* Markoff & Schwartz, *supra* note 4.

79. *See Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?: Hearing Before the Subcomm. on Oversight and Investigations of the House Comm. on Energy and Commerce*, 107th Cong., statement of Sallie McDonald, Assistant Commissioner, USGSA, *available at* http://www.nist.gov/hearings/2001/govcomp.htm (Apr. 5, 2001); Vise, *supra* note 71.

80. *See* Todd R. Weiss, *Denial-of-Service Warning Put Out by FBI Cybercrime Agency*, COMPUTERWORLD, *at* www.computerworld.com/cwi/story/0,1199,NAV47_STO60317,00.html (May 7, 2001); Robert Lemos, *Hackers Cripple White House Site*, CNET NEWS, *at* news.cnet.com/news/0-1003-200-5825982.html (May 4, 2001); Robert Lemos, *Internet Warning System Attacked*, CNET NEWS, *at* news.cnet.com/news/0-1003-202-6016900.html (May 23, 2001); *White House Site Hit by Another DoS Attack*, CNET NEWS, *at* news.cnet.com/news/0-1003-200-6044030.html (May 25, 2001); Brian Sullivan, *CERT Officials Downplay Last Week's Attack*, COMPUTERWORLD, *at* www.computerworld.com/cwi/story/0,1199,NAV47_STO60924,00.html (May 29, 2001). *See also* Robert Lemos, *A Year Later, DDoS Attacks Still a Major Web Threat*, CNET NEWS, *at* news.cnet.com/news/0-1003-201-4735597-0.html (Feb. 7, 2001); Robert Lemos, *DDoS Attacks Underscore Net's Vulnerability*, CNET NEWS, *at* news.cnet.com/news/0-1003-200-6158264.html (June 1, 2001).